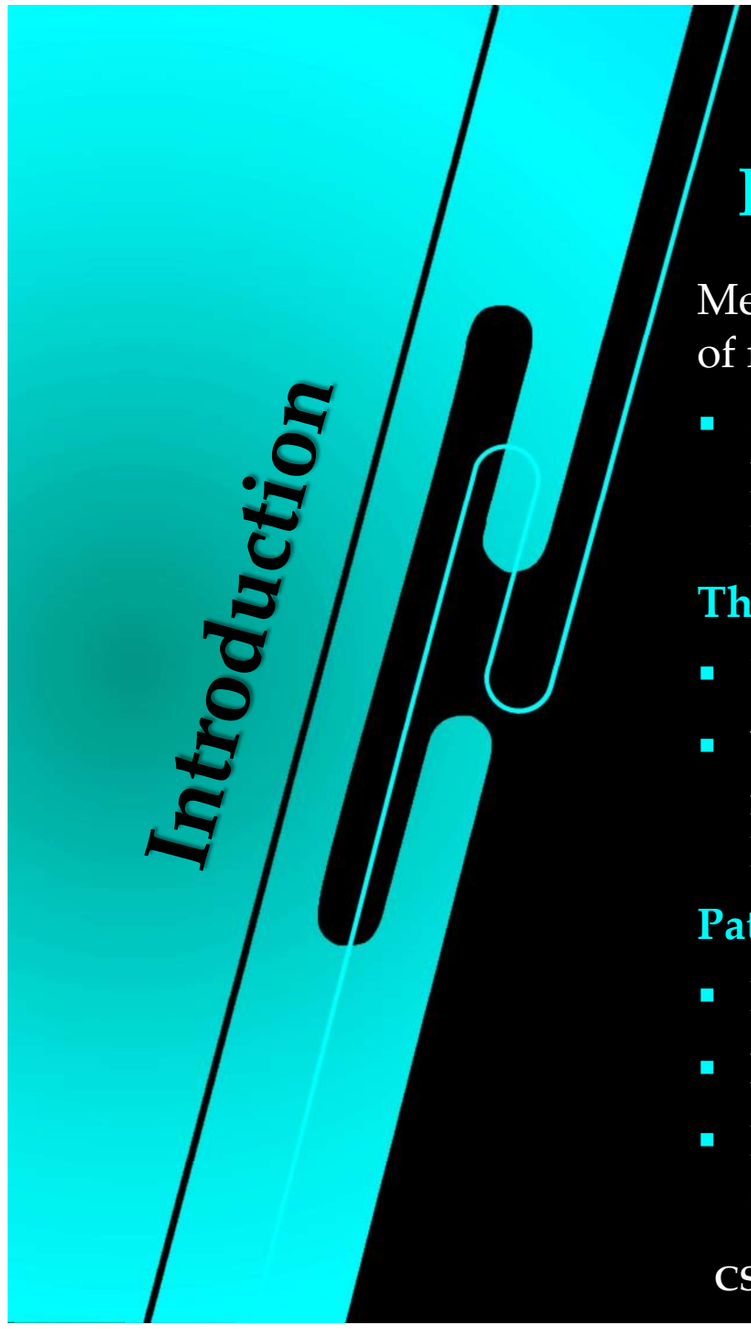
Digital Forensics for Health

CSP012

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Digital Forensics for Health

Introduction



Medical imaging devices have revolutionized patient care. Increased connectivity of modern devices raises cybersecurity concerns.

- **Challenges:** Integrating cybersecurity into equipment development due to long lifecycles. Rapidly evolving cyber threats targeting healthcare pose significant risks. Impact of cyberattacks on patient care and electronic medical records.

The Problem With PACS

- Efficient storage and transmission of patient images and data.
- Vulnerabilities: Default configurations, lack of security measures. Exposure of million medical images in 2019 due to poor security practices (report from ProPublica).

Patient Care and Cybersecurity

- Hospitals face challenges in updating outdated equipment and software.
- Risk of cyberattacks due to unpatched systems.
- Impact of EternalBlue attack on unpatched hospital computers and medical devices.

Healthcare Domain Infrastructure

Assets and Protocols in Healthcare

- **DICOM (Digital Imaging and Communications in Medicine):** DICOM is a standard for transmitting, storing, and sharing medical imaging data such as X-rays, MRIs, and CT scans. It is widely used in healthcare for the exchange of medical images between different systems and facilities.
- **PACS (Picture Archiving and Communication System):** PACS is a system used for storing, retrieving, and distributing medical images. It integrates with DICOM and provides healthcare professionals with access to patient images and related data.
- **HL7 FHIR (Health Level Seven Fast Healthcare Interoperability Resources):** HL7 FHIR is a standard for exchanging electronic healthcare information. It enables interoperability between different healthcare systems and facilitates the exchange of patient data such as medical records, lab results, and clinical observations.
- **Domain Controller - Active Directories:** Active Directory is a directory service developed by Microsoft for managing user identities, permissions, and access to resources within a network. In healthcare organizations, Active Directory is used to manage user accounts, access controls, and authentication.

Digital Forensics for Health

DFH and DFIR

Digital Forensics for Health (DFH) involves investigating digital data in healthcare to ensure cybersecurity and integrity. DFIR (Digital Forensics and Incident Response) is a real-time approach to detecting and mitigating cybersecurity incidents. Both are vital for securing patient information and healthcare IT systems.

Digital Forensics for Health (DFH)

- Investigative process applied to digital data in the healthcare sector.
- Focuses on analyzing digital evidence related to health information systems and medical devices.
- Aims to uncover and mitigate cybersecurity incidents, breaches, or malfunctions within healthcare IT infrastructure.

DFIR (Digital Forensics and Incident Response)

- Integrated approach combining digital forensics and incident response practices.
- Involves detecting, analyzing, and mitigating cybersecurity incidents in real-time.
- Crucial for maintaining the integrity and security of digital assets and systems in various sectors, including healthcare.

DFH and DFIR

Digital Forensics and Incident Response

What is DFIR?

Digital Forensics and Incident Response (DFIR) is a multidisciplinary field within cybersecurity dedicated to identifying, collecting, preserving, examining, and analyzing digital evidence related to computer systems, networks, and digital devices.

- **Example 1:** In the event of a data breach, DFIR specialists analyze logs, metadata, and network traffic to trace the source of the breach, determine the extent of unauthorized access, and identify the compromised data.
- **Example 2:** During a cyberattack investigation, DFIR experts use forensic tools to extract and analyze artifacts from compromised devices to understand the attacker's tactics and motives.

Digital Forensics

This aspect involves the systematic and scientific examination of digital artifacts to reconstruct events, establish timelines, and uncover the source and impact of cyber incidents.

- **Example 1:** Recovering deleted files or email messages to gather evidence of unauthorized access or data tampering.
- **Example 2:** Analyzing memory dumps to identify malicious processes or malware residing in the system.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com